Exec-SearchPath-01

Path-searching Exec functions are susceptible to malicious programs inserted into the search path

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-22

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 8329 bytes

<table>
<tr><td><b>Attack Category</b></td><td>• Path spoofing or confusion problem
• Malicious Input</td></tr>
<tr><td><b>Vulnerability Category</b></td><td>• Indeterminate File/Path
• Process management</td></tr>
<tr><td><b>Software Context</b></td><td>• Process Management</td></tr>
<tr><td><b>Location</b></td><td></td></tr>
<tr><td><b>Description</b></td><td>Path-searching Exec functions are susceptible to malicious programs inserted into the search path.
The APIs execlp, execvp, popen, and system are usually implemented through a shell or exhibit shell-like characteristics. If user input can affect the arguments to the function a malicious user could change or add commands to be run.
These functions search the path if a full path to the program is not specified. When using these functions always specify the full path to the program. The Windows _exec and system family of functions is also vulnerable in the same manner. Also be sure to include the file extension (.exe, .com, .bat) to prevent unwanted matches.</td></tr>
<tr><td><b>APIs</b></td><td><table>
<tr><th>Function Name</th><th>Comments</th></tr>
<tr><td>_execl</td><td></td></tr>
<tr><td>_execle</td><td></td></tr>
<tr><td>_execlp</td><td></td></tr>
<tr><td>_execlpe</td><td></td></tr>
<tr><td>_execv</td><td></td></tr>
<tr><td>_execvp</td><td></td></tr>
<tr><td>_execvpe</td><td></td></tr>
</table></td></tr>
</table>

[1] http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

_spawnl	
_spawnle	
_spawnlp	
_spawnlpe	
_spawnv	
_spawnve	
_spawnvp	
_spawnvpe	
_texecl	
_texecle	
_texeclp	
_texeclpe	
_texecv	
_texecve	
_texecvp	
_texecvpe	
_tspawnl	
_tspawnle	
_tspawnlp	
_tspawnlpe	
_tspawnv	
_tspawnve	
_tspawnvp	
_tspawnvpe	
_wexecl	
_wexecle	
_wexeclp	
_wexeclpe	

_wexecv	
_wexecve	
_wexecvp	
_wexecvpe	
_wspawnl	
_wspawnle	
_wspawnlp	
_wspawnlp	
_wspawnlpe	
_wspawnv	
_wspawnve	
_wspawnvp	
_wspawnvpe	
_wsystem	
execlp	
exect	
execvp	
popen	
system	

Method of Attack	These functions will search the path for the first match to the specified program and are thus susceptible to path spoofing attacks. Additionally, on Windows platforms, these functions will execute a .com program before a .exe program unless the file extension is fully specified. This could allow an attacker to place a malicious .com program in the same location as a similar .exe program.
Exception Criteria	
Solutions	

Solution Applicability	**Solution Description**	**Solution Efficacy**
When any type of path-searching Exec function is used.	When using these functions always specify the full path to the program.	Effective.

	Also be sure to include the file extension (.exe, .com, .bat) on Windows platforms to prevent unwanted searches.
Signature Details	Any of the indicated APIs, with a non-absolute path or (on Windows) no explicit file extension.
Examples of Incorrect Code	`system("MyProgram");`
Examples of Corrected Code	`system("/usr/local/bin/MyProgram");`
Source References	• Viega, John & McGraw, Gary. *Building Secure Software: How to Avoid Security Problems the Right Way*. Boston, MA: Addison-Wesley Professional, 2001, ISBN: 020172152X, pg. 322 • man pages for execlp, execvp, popen, and system • Microsoft Developer Network Library
Recommended Resource	
Discriminant Set	**Operating Systems**: • Windows (All) • UNIX (All) **Language**:

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com